Форма № Н - 3.04

Національний університет біоресурсів і природокористування України
Кафедра комп'ютерних систем, мереж та кібербезпеки

«ЗАТВЕРДЖУЮ»

Декан факультету
інформаційних технологій
_____ проф. О.Г. Глазунова
«___» _____ 2022р.

СХВАЛЕНО
на засіданні кафедри
комп'ютерних систем,
мереж та кібербезпеки
Протокол №12 від «11» травня» 2022р.
Завідувач кафедри
(проф. Лахно В.А.)

РОЗГЛЯНУТО
Гарант ОП «Кібербезпека»
_____ (Лахно В.А.)

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

"Основи аудиту інформаційної безпеки"

зі спеціальності 125 – «Кібербезпека»
(шифр і назва напряму підготовки)

Освітня програма «Кібербезпека»

факультет інформаційних технологій
(назва факультету)

Київ – 2022 р.

Опис навчальної дисципліни
Основи аудиту інформаційної безпеки
(назва)

Галузь знань, напрям підготовки, спеціальність, освітньо-кваліфікаційний рівень		
Галузь знань	Інформаційні технології	
Спеціальність	125 – «Кібербезпека»	
другий (магістерський) рівень	Бакалавр	
Характеристика навчальної дисципліни		
Вид	вибіркова	
Загальна кількість годин	120	
Кількість кредитів ECTS	4	
Кількість змістових модулів	7	
Курсовий проект (робота) (якщо є в робочому навчальному плані)	-	
Форма контролю	Іспит	
Показники навчальної дисципліни для денної та заочної форм навчання		
	денна форма навчання	заочна форма навчання
Рік підготовки	2022-2023	
Семестр	2	
Лекційні заняття	30 год.	
Практичні, семінарські заняття		
Лабораторні заняття	30 год.	
Самостійна робота	60 год.	
Індивідуальні завдання		
Кількість тижневих годин для денної форми навчання: аудиторних	4 год.	

1. Мета та завдання навчальної дисципліни

Курс має навчити майбутніх спеціалістів навчитися відповідати вимогам інформаційної безпеки - це комплексний, циклічний процес, який складається з наступних етапів: - планування аудиту; - планування заходів по аудиту (розробка, узгодження і затвердження планів заходів); - перевірка на відповідність групі вимог (наприклад, на відповідність стандарту ISO/IEC 27001: 2013); - систематизація результатів обстеження і формування звітності.

Набуття компетентностей:

Відповідно до освітньої програми підготовки фахівців за спеціальністю 125 «Кібербезпека» навчальна дисципліна забезпечує формування загальних і фахових компетентностей:

Загальні компетентності:

КЗ 2. Знання та розуміння предметної області та розуміння професії.

КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.

КЗ 8. Здатність до абстрактного і системного мислення, аналізу та синтезу..

Спеціальні (фахові) компетентності:

СК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.

СК7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).

СК8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.

СК12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

В результаті вивчення навчальної дисципліни студент набуде певні програмні результати, а саме:

ПРН 7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки;

ПРН 8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки;

ПРН 9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки;

ПРН 22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки;

ПРН 28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки;

ПРН 39. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах;

ПРН 41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур.

Навчальна програма розрахована на здобувачів вищої освіти, які навчаються за освітньою програмою підготовки бакалаврів за спеціальністю 125 «Кібербезпека».

Робоча програма побудована за вимогами кредитно-модульної системи організації навчального процесу у закладах вищої освіти і використанням академічної системи оцінювання досягнень студентів та шкали оцінок Європейської кредитно-трансферної системи (ECTS).

Навчальна програма розроблена на підставі наступних документів:

-освітньо-професійна програма підготовки фахівців за спеціальністю «Кібербезпека»;

-навчальний план підготовки бакалаврів за спеціальністю «Кібербезпека».

Навчальна програма характеризує шляхи перетворення інформації, що одержується студентом впродовж вивчання курсу, і відбиває зміст курсу, розподілення його на розділи та їх обсяги, дані про форми вивчення та контролю знань.

Теоретичною базою для вивчення є курс «Організаційне забезпечення захисту інформації».

2. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин											
	денна форма						Заочна форма					
	усього	у тому числі					усього	у тому числі				
		л	п	лаб	інд	с.р.		л	п	лаб	інд	с.р.
1	2	3	4	5	6	7	8	9	10	11	12	13
Змістовий модуль 1. Основні види аудиту інформаційної безпеки. Експертний аудит.												
Тема №1. Системи аудиту інформаційної безпеки.	7	2		0		5						
Тема №2. Системи менеджменту інформаційної безпеки (СМІБ) за вимогами ISO/IEC 27001.	11	2		4		5						
Тема №3. Стандарт CobiT 4.1.	11	2		4		5						
Тема №4. Стандарт ISO/IEC 15408. Серія стандартів ISO/IEC 2700X.	9	2		2		5						
Тема №5. Комплексний аудит інформаційної безпеки Компетентність особи, що здійснює управління програмою аудиту.	9	2		2		5						
Тема №6. Оцінка діяльності з управління інформаційною безпекою організації.	9	2		2		5						
Разом за змістовим модулем 1	**56**	**12**		**14**		**30**						
Змістовий модуль 2. Управління інцидентами інформаційної безпеки.												
Тема № 7. Базові принципи, терміни та визначення системи менеджменту інцидентами інформаційної безпеки (СМІБ).	9	2		2		5						
Тема №8. Етапи управління інцидентами інформаційної безпеки відповідно до ISO/IEC 27035.	7	2		0		5						
Тема № 9. Особливості менеджменту інцидентів відповідно до ITIL.	13	2		6		5						
Тема № 10. Концепція та структура автоматизованої системи управління інцидентами інформаційної безпеки.	11	4		2		5						
Тема № 11. Функціонування груп реагування на інциденти інформаційної безпеки CERT/CSIRT.	13	4		4		5						
Тема № 12. Обробка інцидентів інформаційної безпеки групами CERT/CSIRT. Документаційне забезпечення процесу управління інцидентами інформаційної безпеки.	11	4		2		5						
Разом за змістовим модулем 2	**64**	**18**		**16**		**30**						
Усього годин за курс	**120**	**30**		**30**		**60**						

4. Теми семінарських занять

№ з/п	Назва теми	Кількість годин
	Не передбачено робочим навчальним планом	

5. Теми практичних занять

№ з/п	Назва теми	Кількість годин
	Не передбачено робочим навчальним планом	

6. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1.	Основні види аудиту інформаційної безпеки. Експертний аудит. Активний аудит.	4
2.	Склад процедури аудиту. Критерії аудиту. Процес усвідомлення аудиту інформаційної безпеки. Програма аудиту інформаційної безпеки.	4
3.	Алгоритм організації та проведення внутрішніх аудитів. Пошук загроз.	4
4.	Моделювання загроз. Позаплановий внутрішній аудит.	4
5.	Розробка процедур для програми аудиту. Визначення ресурсів, необхідних для реалізації програми аудиту.	6
6.	Ознаки інциденту інформаційної безпеки. Аналіз інцидентів інформаційної безпеки.	4
7.	Основні етапи управління інцидентами відповідно до ITIL. Варіанти категорування інцидентів відповідно до ITIL.	4
	Разом	**30**

7. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	Оцінка діяльності з управління інформаційною безпекою організації.	5
2	Основні заходи створення СМІБ. Ознаки інциденту інформаційної безпеки.	5
3	Етапи управління інцидентами інформаційної безпеки відповідно до ISO/IEC 27035.	5
4	Місце процесу управління інцидентами серед усіх процесів ITIL. Основні етапи управління інцидентами відповідно до ITIL.	5
5	Сховище інформації про ІІБ. Аналітичні інструменти і засоби генерації звітів.	5
6	Усунення причин, наслідків інциденту і його розслідування.	5
7	Загальна характеристика діяльності груп CERT/CSIRT.	5
8	Документаційне забезпечення процесу управління інцидентами інформаційної безпеки.	5
9	Стандарти, рекомендації та кращі світові практики щодо управління інцидентами інформаційної безпеки.	5
10	Аналіз інцидентів інформаційної безпеки.	5
11	Аналіз та удосконалення програми аудиту.	5
12	Принципи проведення внутрішнього аудиту. Дев’ять правил успішного проведення аудиту.	5
	Разом	**60**

8. Контрольні питання для перевірки знань студентів (приклади питань)

1. Системи аудиту інформаційної безпеки.
2. Основні види аудиту інформаційної безпеки. Експертний аудит.
3. Активний аудит.
4. Аудит на відповідність стандартам інформаційної безпеки.
5. Діагностичний аналіз Системи менеджменту інформаційної безпеки (СМІБ) за вимогами ISO/IEC 27001.
6. Внутрішній аудит СМІБ.
7. Завдання аудиту. Мета аудиту. Склад процедури аудиту. Критерії аудиту.
8. Процес усвідомлення аудиту інформаційної безпеки. Програма аудиту інформаційної безпеки. Принципи проведення аудиту.

– Стандарт CobiT 4.1. Бібліотека інфраструктури інформаційних технологій ITIL. Стандарт ISO/IEC 15408. Серія стандартів ISO/IEC 2700X.

9. Загальна характеристика внутрішніх аудитів СМІБ. Принципи проведення внутрішнього аудиту. Алгоритм організації та проведення внутрішніх аудитів.
10. Пошук загроз. Моделювання загроз.
11. Позаплановий внутрішній аудит. Приклад вимог до процедур з внутрішнього аудиту. Принципи проведення внутрішнього аудиту.
12. Дев’ять правил успішного проведення аудиту. Управління програмою аудиту.
13. Розробка цілей програми аудиту. Розробка програми аудиту.
14. Комплексний аудит інформаційної безпеки
15. Компетентність особи, що здійснює управління програмою аудиту.
16. Встановлення обсягу програми аудиту. Виявлення та оцінювання ризиків для програми аудиту. Розробка процедур для програми аудиту.
17. Визначення ресурсів, необхідних для реалізації програми аудиту. Реалізація програми аудиту.
18. Вибір методів проведення аудиту.
19. Формування команди з аудиту.
20. Моніторинг програми аудиту.
21. Аналіз та удосконалення програми аудиту.
22. Оцінка діяльності з управління інформаційною безпекою організації
23. Встановлення цілей, сфери та критеріїв для конкретного аудиту.
24. Покладання відповідальності на керівника команди з аудиту за конкретний аудит.
25. Управління результатами реалізації програми аудиту.
26. Використання записів відповідно до програми аудиту та їх збереження.
27. Специфічні знання та навички аудиторів, пов'язані з особливостями систем менеджменту і галузями економіки.
28. Базові принципи, терміни та визначення системи менеджменту інцидентами інформаційної безпеки (СМІІБ).
29. Цілі управління інцидентами. Основні заходи створення СМІІБ.
30. Ознаки інциденту інформаційної безпеки.
31. Аналіз інцидентів інформаційної безпеки.
32. Визначення показників ефективності процесу управління інцидентами інформаційної безпеки.
33. Етапи управління інцидентами інформаційної безпеки відповідно до ISO/IEC 27035
34. Етапи формування СМІІБ відповідно до моделі PDCA.
35. Модель життєвого циклу процесу УІІБ. Усунення причин, наслідків інциденту і його розслідування.
36. Місце процесу управління інцидентами серед усіх процесів ITIL.
37. Основні етапи управління інцидентами відповідно до ITIL.
38. Варіанти категорування інцидентів відповідно до ITIL.
39. Інтеграційна платформа автоматизованої системи управління інцидентами інформаційної безпеки.
40. Апаратно-програмні засоби моніторингу і аудиту.
41. Апаратно-програмні засоби захисту.
42. Сховище інформації про ІІБ. Аналітичні інструменти і засоби генерації звітів.
43. Функціонування груп реагування на інциденти інформаційної безпеки CERT/CSIRT.
44. Сервіси, що надаються групами реагування на інциденти інформаційної безпеки. Обробка інцидентів інформаційної безпеки групами CERT/CSIRT.
45. Документаційне забезпечення процесу управління інцидентами інформаційної безпеки.

9. Методи навчання

Проведення лекцій з використанням технічних засобів навчання.

Виконання лабораторних робіт з використанням наочних технічних засобів навчання у вигляді систем моделювання за допомогою інженерних пакетів проектування цифрових пристроїв. Проведення самостійної роботи засобами інформаційно-комунікаційних технологій в освіті. Використовується електронний навчальний курс на платформі Moodle.

10. Форми контролю

Захист результатів виконання лабораторних робіт.

Контрольне тестування відповідно до кожного змістовного модуля, що створений у комп'ютерному навчальному середовищі.

Підсумкова атестація: іспит.

11. Розподіл балів, які отримують студенти

Оцінювання знань студента відбувається за 100-бальною шкалою і переводиться в національні оцінки згідно з табл.1 «Положення про екзамени та заліки у НУБіП України» (наказ про уведення в дію від 27.12.2019 р. № 1371):

Рейтинг здобувача вищої освіти, бали	**Оцінка національна за результати складання екзаменів заліків**	
	Екзамен	**Залік**
90-100	Відмінно	зараховано
74-89	Добре	
60-73	Задовільно	
0-59	незадовільно	не зараховано

Для визначення рейтингу студента із засвоєння дисципліни $R_{дис}$ (до 100 балів) одержаний рейтинг з атестації $R_{АТ}$ (до 30 балів) додається до рейтингу студента з навчальної роботи $R_{НР}$ (до 70 балів): $R_{дис}=R_{НР}+R_{АТ}$.

12. Методичне забезпечення

Електронний навчальний курс на платформі Moodle вміщує методичне забезпечення включаючи: лекції, презентації до лекцій, методичні вказівки до виконання лабораторних робіт, глосарій термінів тощо.

13. Рекомендована література

Базова

1.Корченко О.Г. Аудит та управління інцидентами інформаційної безпеки // О.Г. Корченко, С.О. Гнатюк, С.В. Казмірчук, В.М. Панченко, С.В. Мельник. – К.: Центр навч.-наук. та наук.-пр. видань НА СБ України, 2014. – 193 с.

Допоміжна

1. Кузнецов О. О. Захист інформації в інформаційних системах. Методи традиційної криптографії / О.О. Кузнецов, С.П. Євсеєв, О.Г. Король. – Х.: Вид. ХНЕУ, 2010. – 316 с.

2. Браіловський М.М. Захист інформації у банківській діяльності / М.М. Браіловський, Г.П. Лазарєв, В.О. Хорошко. – К.: ТОВ "ПоліграфКонсалтинг", 2010. – 216 с.

3. Herrmann D.S. Complete Guide to Security and Privacy Metrics: Measuring Regulatory Compliance, Operational Resilience, and ROI / D.S. Herrmann. – Auerbach Publications. – 2007. – 824 p.

4. Jansen W. Directions in Security Metrics Research. NISTIR 7564. [Електронний ресурс] // Режим доступу: http://csrc.nist.gov/publications/nistir /ir7564/nistir-7564_metrics-research.pdf.

5. Information technology. Security techniques. Information security incident management: ISO 27035:2011. – 78 p.

6. Юдін О.І. Захист інформації в мережах передачі даних // О.І. Юдін, О.Г. Корченко, Г.Ф. Конахович – К.: Вид-во ТОВ «НВП» Інтерсервіс», 2009. – 716 с.

14. Інформаційні ресурси

1. ДСТУ ISO/IEC 11770-3:2002 «Інформаційні технології. Методи захисту».
2. НД ТЗІ 1.1-005-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.
3. НД ТЗІ 1.4-001-00. Типове положення про службу захисту інформації в автоматизованій системі.